UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/610,722	07/06/2000	Suresh Krishna	BRCMP005	5437

28393 7590 11/07/2006

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVE., N.W.
WASHINGTON, DC 20005

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 11/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/610,722	KRISHNA ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *46-70* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *46-70* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/25/2006 has been entered.

Response to Arguments

2. In response to communications filed on 8/25/2006, applicant has amended claims 46-65. The following claims 46-70 are presented for examination.

2.1 Applicant's arguments, filed on 8/25/2006, with respect to the rejection of claims 46-70 have been fully considered, but they are not persuasive. Applicant argues that the server in Leung does not include a plurality of processing engines for performing authentication. Examiner respectfully disagrees. Leung discloses that the server may be a centralized server that may provide authentication services and authorization services (see column 6, lines 29-38). It is well known in the art for a server to include plurality of processing engines to perform operations in parallel and the server of Leung is configured for providing services for plurality of mobile nodes. Applicant has amended the claims to replace the word "system" by "device" and to more particularly point out that the processing engines are in the device. It only requires routine skill in the art to combine processes that can be performed by two or more machines into one machine

In re Japikse 86 USPQ 70 (CCPA 1950). Applicant has not overcome the rejection as explained above. Upon further consideration, claims 46-70 are now rejected in view of Leung and Harrison et al (Applicant's disclosure).

Information Disclosure Statement

3. The information disclosure statements (IDS) submitted on 8/25/2006 and 9/25/2006 were filed in a continuation application. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements are being considered by the examiner.

Claim Objections

4. Claim 56 is objected to because of the following informalities: claim 56 recites "contact addressable memory" which is interpreted by the Examiner as "content addressable memory" since CAM stands for "content addressable memory". Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5.1 Claims 58-59 and 61-62 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Applicant's disclosure does not explicitly describe the device, as claimed in claim 46, being a router, firewall, gateway, or server. The specification on the other hand merely states that the cryptography accelerator chips (processing engines) may be included in routers or gateways (see Applicant's background, page 1, lines 19-25). Also, there is no disclosure of the device being a firewall nor a server.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 46-70 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,760,444 to **Leung** in view of European Patent Publication EP-0876026 A2 to **Harrison et al**

(Applicant's IDS).

As per claim 46, **Leung** discloses a server (device) comprising: a classification module in the device that determines security association information associated with each data packet in a plurality of data packets, for example (see column 7, lines 33-50); wherein the classification module is configured to provide at least a portion of the security information associated with the packets to a plurality of security processing engines, for example (see column 7, lines 33-50; column 6, lines 7-46; column 4, lines 32-62; and claims 1-3) that perform authentication and cryptographic operations. **Leung** discloses in one embodiment home agents performing hashing or message digest authentication using cryptographic keys that include encryption/decryption operations (see column 3, lines 15-45 and column 3, line 45 through column 4, line 5). As described above, **Leung** discloses plurality of processing engines are configured to process plurality of data packets in parallel; in another embodiment, **Leung** discloses a server performing the determining step and authentication and cryptographic operations (column 8, line 36 through column 9, line 15 and column 7, lines 15-21) that also meets the recitation of wherein the plurality of processing engines in the device are configured to process plurality of data packets in parallel. Although **Leung** discloses that the server may perform many authentication operations, **Leung** is silent about the processing being done by many processors in the server, it is implicit that the server has plurality of processors for performing the invention disclosed. And it would have been an obvious modification to one of ordinary skill in the art to use plurality of processing engines to perform the process in parallel as to improve latency and performance. **Harrison et al** in an analogous art teaches plurality of processing engines configured to process

plurality of data packets in parallel and to provide significantly improved performance for functions such as encryption, decryption, and other secure services such as message authentication, message signature, and others (see abstract and column 20, lines 35-58); and discloses a system and method that supports multiple programs using a single ULSI design (see abstract and column 3, lines 25-50; and column 20, lines 35-58); and suitable for concurrently processing multiple cryptographic programs (see column 5, lines 13-32; 50-58; column 19, lines 25-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the authentication and authorization functions of the server in **Leung** into one single device using plurality of processing engines configured to process plurality of data packets in parallel. The motivation to do so is given by **Harrison et al** who teaches plurality of processing engines in one single device for providing many advantages such as significantly improving performance for cryptographic functions and authentication; suitable for concurrently processing multiple cryptographic programs. **Harrison et al** adds that using one single integrated circuit device significantly reduces security risk because key variable data is vulnerable when exchanged between subsystems (see column 20, lines 45-58).

As per claims 47-48, the references as combined above disclose the limitation of further comprising a database including security association information wherein the database is local to the classification module, and wherein the database includes one or more entries wherein each entry defines information associated with one security association, for example (see **Leung**, column 3, line 45 through column 4, line 31 and column 6, lines 7-32).

As per claim 49, the references as combined above disclose the limitation of wherein the database is located on the same chip as the classification module, for example (see **Leung**, column 9, lines 21-52; and **Harrison et al**, column 20, lines 45-58).

As per claim 50, the references as combined above disclose the limitation of wherein the security association information includes a sequence number an anti-replay window and a lifetime of the security association, for example (see **Leung**, column 3, line 45 through column 4, line 5).

As per claim 51, the references as combined above disclose the limitation of wherein the security association information further includes an encapsulating security payload (ESP) encryption algorithm identifier and one or more ESP encryption keys, for example (see **Leung**, column 3, line 45 through column 4, line 5).

As per claims 52-53, the references as combined above disclose the limitation of wherein the security association information further includes an (ESP) authentication algorithm identifier and one or more ESP authentication keys and an authentication header (AH) authentication algorithm identifier and one or more AH authentication keys, for example (see **Leung**, column 3, line 1 through column 4, line 5).

As per claim 54, the references as combined above disclose the limitation of wherein the security association information includes protocol mode information, for example (see **Leung**, column 2, line 58-column 3, line 15 and column 3, lines 45-65).

As per claim 55, the references as combined above disclose wherein the database is stored in memory (see **Leung**, column 10, lines 40-55).

As per claim 56, the references as combined above disclose the claimed device of claim 55 and discloses that the invention may be performed using any type of memory or data storage (see **Leung**, column 9, lines 15-22). Leung does not explicitly disclose that the memory is content addressable memory. A content addressable memory (CAM) is well known in the art for very fast table lookups since the data items are not accessed based on memory address or location but by analysis of content. Therefore, it would have been an obvious modification to one of ordinary skill in the art to use such memory for very fast table lookups.

As per claim 57, the references as combined above disclose the claimed device of claim 55 and further discloses wherein the memory is random-access memory (see **Leung**, column 9, lines 15-22).

As per claims 58-59 and 61, the references as combined above disclose the claimed device of claim 46. It is obvious to one of ordinary skill in the art that the invention as combined above can be implemented in different communication device such as router, firewall,

or gateway device to provide routing table computations and network management (see **Leung**, column 9, lines 39-41 and column 10, lines 25-39).

As per claim 60, the references as combined above disclose the claimed device of claim 46 and further discloses wherein the device is a network communication device (see **Leung**, column 6, lines 24-28).

As per claim 62, the references as combined above disclose the claimed device of claim 46 and further discloses wherein the device is a server (see **Leung**, column 6, lines 24-28).

As per claim 63, the references as combined above disclose the limitation of wherein the device is a network line card, for example (see **Leung**, column 35-52; and **Harrison et al**, column 20, lines 45-58).

As per claim 64, **Leung** discloses a method for classifying data packets during security processing in a server (device) comprising: receiving a packet identifying a mobile node and obtaining security association from a security association table, the server is configured to construct the packet and includes security association and provides at least a portion of the security association to at least one of a plurality of Home Agents or processors in the server (processing engines) that perform authentication and cryptographic operations that meets the recitation of receiving in the device at least a portion of a header for each data packet in a plurality of data packets (see column 7, lines 33-50 and column 2, line 57 through column 3, line

15); determining security association information associated with each data packet in a plurality of data packets, for example (see column 7, lines 33-50); providing at least a portion of the security information associated with the packets to a corresponding security processing engine in a plurality of security processing engines, for example (see column 7, lines 33-50; column 6, lines 7-46; column 4, lines 32-62; and claims 1-3) that perform authentication and cryptographic operations. **Leung** further discloses home agents performing hashing or message digest authentication using cryptographic keys that include encryption/decryption operations (see column 3, lines 15-45 and column 3, line 45 through column 4, line 5). As described above, **Leung** discloses plurality of processing engines are configured to process plurality of data packets in parallel; in another embodiment, **Leung** discloses a server performing the determining step and authentication and cryptographic operations (column 8, line 36 through column 9, line 15 and column 7, lines 15-21) that also meets the recitation of wherein the plurality of processing engines in the device are configured to process plurality of data packets in parallel. Although **Leung** discloses that the server may perform many authentication operations, **Leung** is silent about the processing being done by many processors in the server, it is implicit that the server has plurality of processors for performing the invention disclosed. And it would have been an obvious modification to one of ordinary skill in the art to use plurality of processing engines to perform the process in parallel as to improve latency and performance. **Harrison et al** in an analogous art teaches plurality of processing engines configured to process plurality of data packets in parallel and to provide significantly improved performance for functions such as encryption, decryption, and other secure services such as message authentication, message signature, and others (see abstract and column 20, lines 35-58); and discloses a system and

method that supports multiple programs using a single ULSI design (see abstract and column 3, lines 25-50; and column 20, lines 35-58); and suitable for concurrently processing multiple cryptographic programs (see column 5, lines 13-32; 50-58; column 19, lines 25-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the authentication and authorization functions of the server in Leung using plurality of processing engines in one single device configured to process plurality of data packets in parallel. The motivation to do so is given by **Harrison et al** who teaches plurality of processing engines in one single device for providing many advantages such as significantly improving performance for cryptographic functions and authentication; suitable for concurrently processing multiple cryptographic programs. **Harrison et al** adds that using one single integrated circuit device significantly reduces security risk because key variable data is vulnerable when exchanged between subsystems (see column 20, lines 45-58).

As per claims 65-67, the references as combined above disclose the limitation of wherein the step of determining security association information comprises accessing a database to determine security association information (see column 6, lines 13-28) and further comprises using one or more selectors to identify a security association information entry in the database wherein the one or more selectors include at least one of a destination IP address, a security protocol identifier and a security protocol identifier and a security parameter index, for example (see **Leung**, column 7, lines 25-37; column 3, lines 6-12).

As per claims 68-69, the references as combined above disclose the limitation of wherein the one or more selectors include a destination IP address, a source IP address and a transport layer protocol and wherein one or more selectors further include a source port and a destination port (see **Leung**, column 7, lines 25-37 and column 9, line 52 through column 10, line 40) this is well-known in the art as included in IP header for performing IPsec processing and also disclosed in RFC 2401, "Security Architecture for IP" in Applicant's disclosure.

As per claim 70, the references as combined above disclose updating or generating new security association in a database of the server to store security association information for the Home Agent that meets the recitation of wherein the step of determining security association information comprises if no security association information exists in the database associated with the packet, generating the security association information and storing the security association information in an entry in the database, for example (see **Leung**, column 7, line 50 through column 8, line 40).

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carl Colin
Patent Examiner
November 3, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

11/03/06